TECHNISCHE UNIVERSITÄT BERLIN Sommersemester 2004
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. Heß
WM: Dipl.-Math. M. Wagner
`www.math.tu-berlin.de/~hess/krypto`

6. Übung Kryptographie

1. Aufgabe Carmichael-Zahlen (4 Punkte)

Sei $n \in \mathbb{N}$ eine ungerade zusammengesetzte Zahl (d.h für $n = \prod_{i=1}^{m} p_i^{e_i}$ mit $e_i \in \mathbb{N}\backslash\{0\}, p_i \in \mathbb{P}$ gilt $m \geq 2$ oder $e_1 \geq 2$), für die

$$a^{n-1} \equiv 1 \mod n$$

für ein $a \in \mathbb{Z}$ gilt. Solch eine Zahl nennt man **Pseudoprimzahl** zur Basis a. Ist n eine Pseudoprimzahl zur Basis a für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$, dann heißt n **Carmichael-Zahl**. Man nennt ein $n \in \mathbb{N}$ **quadratfrei**, wenn es kein $p \in \mathbb{P}$ gibt mit $p^k | n$ für $k \geq 2$. Für ein zusammengesetztes $n \in \mathbb{N}$ gilt:

$$n \text{ ist Carmichael-Zahl } \Leftrightarrow n \text{ ist quadratfrei und es gilt: } p|n \Rightarrow (p-1)|(n-1) \ (p \in \mathbb{P})$$

Zeigen Sie, daß eine Carmichael-Zahl mindestens drei verschiedene Primteiler hat.

2. Aufgabe Gruppentheorie (6 Punkte)

(i) Sei G eine abelsche Gruppe mit $|G| = p \in \mathbb{P}$. Zeigen Sie, daß G zyklisch ist, d.h. es existiert ein $g \in G$ mit $\langle g \rangle = G$.

(ii) Sei $G \neq \{e\}$ eine endliche abelsche Gruppe und H eine Untergruppe von G für die gilt: $g^2 \in H \ \forall g \in G$. Zeigen Sie, daß dann $(G : H) = 2^j$ $(j \in \mathbb{N}_0)$ ist. Sie können folgende Aussage ohne Beweis benutzen: Ist G eine endliche Gruppe und $p \in \mathbb{P}$ mit $|G| = p \cdot k$, so besitzt G eine Untergruppe der Ordnung p.

(iii) Sei $G := (\mathbb{Z}/p^k\mathbb{Z})^\times$ $(p \in \mathbb{P}, k \geq 2)$ und $J := \{a \in G : \ a^{n-1} \equiv 1 \mod p^k\}$. Zeigen Sie, daß $(J, \cdot)$ eine Untergruppe von G ist und $(G : J) \geq p^{k-1}$ gilt.

(iv) Sei $G := (\mathbb{Z}/9\mathbb{Z})^\times$ und J wie in (iii). Bestimmen Sie $(G : J)$.

3. Aufgabe Chinesischer Restsatz (3 Punkte)

Zeigen Sie, daß für die eulersche $\phi-$Funktion und $n = n_1 \cdot n_2 \in \mathbb{Z}$ gilt:

$$\phi(n) = \phi(n_1 \cdot n_2) = \phi(n_1) \cdot \phi(n_2) \Leftrightarrow \mathrm{ggT}(n_1, n_2) = 1.$$

4. Aufgabe Praktische Aufgabe (7 Punkte)

Eine Bank verschickt eine Nachricht $m \in \mathbb{N}$ an $e \in \mathbb{N}$ verschiedene Kunden. Jeder dieser Kunden besitzt einen sogenannten " öffentlichen" Schlüssel $(n_i, e) \in \mathbb{N}, i \in \{1, \ldots, e\}$, wobei die n_i paarweise teilerfremd zueinander sind. Der Kunde mit dem Schlüssel n_i erhält die Nachricht $c_i \equiv m^e \mod n_i$.

Eine dritte Person war nun in der Lage, alle Nachrichten c_i abzufangen. Da die Tupel (n_i, e) öffentlich sind, weiß diese Person, daß $c_i \equiv m^e \mod n_i$ gilt. Wie kann diese dritte Person m berechnen?

Demonstrieren Sie dies an folgendem Beispiel: Sei $e = 3$, $n_1 = 93389042359234$, $n_2 = 46731153705941$ und $n_3 = 51552591331651$. Ferner sei

$$\begin{aligned} c_1 &\equiv 9328378988512 && \mod n_1 \\ c_2 &\equiv 29268198689829 && \mod n_2 \\ c_3 &\equiv 36123359008905 && \mod n_3. \end{aligned}$$

Schreiben Sie ein KASH-Programm, welches den Klartext m berechnet wenn $m < n_i$ $(i = 1, 2, 3)$ gilt.

Gesamt: 20 Punkte